25(Amended). A method for protecting a digital signal comprising the steps of:

a) **providing a carrier signal; and**

b) **using a random or pseudo-random key to** encode[ing] independent information including a digital watermark into [a]**the** carrier signal [**using a random or pseudo-random key**].

29(Amended). A method for protecting a digital signal comprising:

a) **providing a carrier signal that has been encoded with independent information; and**

b) **using a random or pseudo-random key to** decode[ing] independent information including a digital watermark from [a]**the** carrier signal [**using a random or pseudo-random key**].

33(Amended). The method according to claim 29, further comprising the step of:

[b)] **c)** generating a first derivative encoded signal representing the original carrier signal combined with the encoded independent information, including the digital watermark, wherein the first derivative encoded signal is an arbitrarily close approximation of the original carrier signal.

34(Amended). The method according to claim 33, further comprising the step of:

[c)] **d)** modifying the first derivative encoded signal to produce a second derivative encoded signal, wherein the second derivative encoded signal differs from the

C3 cont

original carrier signal by a greater degree then the first derivative encoded signal differs

from the original carrier signal, as measured by an arbitrary signal metric.

C4

36(Amended).   The method according to claim 29, further comprising the step of:

   [b)] c) decoding a single message bit from a single sample by reading a simple

bit of the single sample as the message bit.

37(Amended).   The method according to claim 29, further comprising the step of:

   [b)] c) decoding a signal message bit from a single sample by mapping the single

sample into a range of sample values which indicate a particular message bit value.

38(Amended).   The method according to claim 29, further comprising the step of:

   [b)] c) decoding a single message bit from a signal spectral value by mapping the

single spectral into a range of spectral values which indicate a particular message bit

value.

39(Amended).   The method according to claim 25, further comprising the step of:

   [b)] c) using a map table to define where watermark information is to be encoded

based on random or pseudo-random masks into the carrier signal, wherein the map table

is defined such that any index of the map table enables encoding of information.

40(Amended). The method according to [according to] claim 25, further comprising the steps of:

[b)] c) selecting a mask set, said mask set including one or more random or pseudo-random series of bits, referred to as masks;

[c)] d) selecting a random or pseudo-random start of message delimiter; and

[d)] e) selecting independent information to be encoded.

41(Amended). The method according to claim 40, further comprising the step of:

[e)] f) generating a message bit stream to be encoded such that the stream includes:

1) the random or pseudo-random start of message delimiter,

2) a number of message bytes to follow the message, and

3) the independent information.

42(Amended). The method according to claim 41, further comprising the step of:

[f)] g) separating an input sample stream into smaller discrete sample windows comprising segments of the input sample stream.

43(Amended). The method according to claim 42, further comprising of the step of:

[g)] h) using positions within the [input] sample window and a position within the input stream to index random or pseudo-random masks and compute a mapping function to determine encoding positions and encode digital watermark information into the [input] sample window.

DC01:243357.1

- 4 -

44(Amended).   The method according to claim 43, further comprising the step of:

[h)] i)   computing a spectral transform of the **[input]** sample window prior to digital watermark data encoding.

45(Amended).   The method according to claim 44, further comprising the step of:

[i)] j)   computing an inverse spectral transform of the encoded spectral transform data after digital watermark data encoding.

46(Amended).   The method according to claim 29, further comprising the steps of:

[b)] c)   selecting a mask set, said mask set including one or more random or pseudo-random series of bits, referred to as masks,

[c)] d)   selecting a random or pseudo-random start of message delimiter; and

[d)] e)   selecting **[independent information]** **an input sample stream** to be **[encoded]** **decoded**.

47(Amended).   The method according to claim 46, further comprising the step of:

[e)] f)   separating **[an]** **the** input sample stream into smaller discrete sample windows comprising segments of the input sample stream.

48(Amended).   The method according to claim 47, further comprising the step of:

[f)] g)   using positions within **one of** the **[input]** sample window**s** and a position within the input stream to index random or pseudo-random masks and compute a

mapping function to determine decoding positions and **to** decode digital watermark information **from** [into] the [input] sample window.

49(Amended).   The method according to claim 48, further comprising the step of:

[g)] **h)** computing a spectral transform of the [input] sample window prior to digital watermark data [encoding]**decoding**.

$C4$
C cont

51(Amended).   The method according to claim 48, further comprising the step of:

[g)] **h)** validating at least one selected from the group consisting of:

(1) a hash value computed on the start of message delimiter, and

(2) a digital signature of the start of message delimiter,

$C5$

wherein the step [g)] **h)** of validating occurs after the start of message delimiter and the encoded information of said hash value or said digital signature have been decoded and the validation consists of computing an appropriate result using the start of message delimiter, comparing it to a value in the decoded data, and verifying any signature.

52(Amended).   The method according to claim 25, further comprising the step of:

[b)] **c)** adding unique data to each individual watermark, rendering it distinct from any other watermark in the same sample stream.

53(Amended).   The method according to claim 52, further comprising the step of:

[c)] **d)** pre-processing sample windows in the sample stream to be watermarked.

DC01:243357.1

54(Amended).   The method according to claim 53, further comprising the step of:

[d)] e) determining which sample windows will contain the individual digital watermark to be encoded.

55(Amended).   The method according to claim 54, further comprising the step of:

[e)] f) calculating a size of the independent information comprising the digital watermark plus a size of an added hash value to determine a number of sample windows required to contain a complete watermark.

56(Amended).   The method according to claim 55, further comprising the step of:

[f)] g) computing a secure one way hash function of the carrier signal data in said sample windows, wherein said hash function is insensitive to changes introduced into the carrier signal for the purpose of carrying digital watermark information.

57(Amended).   The method according to claim 56, further comprising the step of:

[g)] h) concatenating the hash value with the independent information, creating an expanded, unique digital watermark.

58(Amended).   The method according to claim 29, further comprising the step of:

[b)] c) obtaining a unique hash value contained in the independent information comprising part of the digital watermark.